Journal of Siberian Federal University. Mathematics & Physics 2019, 12(3), 331–341

УДК 511.52

An Elementary Algorithm for Solving a Diophantine Equation of Degree Fourth with Runge's Condition

Nikolai N. Osipov*
Institute of Space and Information Technology
Siberian Federal University
Kirenskogo, 26, Krasnoyarsk, 660074
Russia

Maria I. Medvedeva†
Institute of Space and Information Technology
Siberian Federal University
Kirenskogo, 26, Krasnoyarsk, 660074
Russia

Received 16.08.2018, received in revised form 18.10.2018, accepted 01.04.2019

We propose an elementary algorithm for solving the diophantine equation

$$(p(x,y)+a_1x+b_1y)(p(x,y)+a_2x+b_2y)-dp(x,y)-a_3x-b_3y-c=0 \qquad (*)$$

where $p(x,y)$ denotes an irreducible quadratic form of positive discriminant and $(a_1,b_1)\neq(a_2,b_2)$. The last condition provides that the equation $(*)$ can be solved using the well-known Runge's method, but we prefer to avoid the use of any power series that leads to the upper bounds for solutions which is useless for a computer implementation.

Keywords: diophantine equations, elementary version of Runge's method.

Introduction

As well known, there is a wide class of diophantine equations in two unknowns

$$f(x,y)=0, \qquad (1)$$

for which exists an *effective* solving method (that gives some explicit upper bounds for solutions), the so-called *Runge's method* [7]. A description of the standard version of Runge's method can be found in the well-known monographs [2] and [9] (also see *Theorem of Runge* below).

However, the practical implementation of Runge's method is absent in modern computer algebra systems, with the exception of some special cases (see, e.g., [6, 10]). The original version of Runge's method is based on the Puiseux series of the branches of the algebraic function $y=\Psi(x)$ defined by (1). Unfortunately, this leads to "bad" (too large, see [11]) estimates for the solutions which makes a computer implementation of this method to be difficult. It seems that the realistic (practically working) algorithms for solving diophantine equations (1) with Runge's condition must be based on some other ideas.

*nnosipov@rambler.ru
†mimedvedeva@rambler.com

Let us recall the main result underlying Runge's method. We suppose that the polynomial

$$f(x,y) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_{ij}x^i y^j \in \mathbb{Z}[x,y] \tag{2}$$

with $m = \deg_x f(x,y)$ and $n = \deg_y f(x,y)$ is irreducible over $\mathbb{Q}$. Denote by L the line defined on $\mathbb{R}^2$ by the equation $x/m + y/n = 1$ and by S the set of all (i,j) such that $a_{ij} \neq 0$. In 1887 Carl Runge proved the following theorem (see [7] and, for useful comments, [1, 11]).

Theorem of Runge. Suppose that the equation (1) has infinitely many solutions over $\mathbb{Z}$. Then each of the following conditions holds:

(a) there are no points of S lying above the line L,

(b) the L-leading part

$$f_L(x,y) = \sum_{(i,j)\in S\cap L} a_{ij}x^i y^j$$

is (up to a constant factor) a power of an irreducible over $\mathbb{Q}$ polynomial $p(x,y) \in \mathbb{Z}[x,y]$, and

(c) all the Puiseux expansions of $y = \Psi(x)$ at $x = \infty$ are pairwise conjugate.

We say that a polynomial $f(x,y)$ satisfies *Runge's condition*, if at least one of the conditions (a), (b) or (c) does not hold. Theorem of Runge can be reformulated in the following equivalent form: if $f(x,y)$ satisfies Runge's condition, then the equation (1) has a finite set of solutions over $\mathbb{Z}$. In addition, the proof is constructive and leads to some explicit estimates for the size of integer solutions (see [11, 8] for detailed information; as we noted above, these estimates are useless for a computer implementation even in the case of small m and n).

Rewrite the polynomial (2) as

$$f(x,y) = f_d(x,y) + f_{<d}(x,y),$$

where $d = \deg f(x,y)$ and $f_d(x,y)$ denotes the *leading homogeneous part* of $f(x,y)$. The most known, but simplified version of Theorem of Runge is the following (see, e.g., [2, Ch. 28]).

Corollary. If $f_d(x,y)$ can be decomposed into a product of non-constant relatively prime polynomials in $\mathbb{Z}[x,y]$, then the equation (1) has a finite set of solutions over $\mathbb{Z}$.

Proof. Clearly, $d \geqslant \max\{m,n\}$. The condition on $f_d(x,y)$ implies that either (a) or (b) is not satisfied. □

Assuming the condition of Corollary to be satisfied, for the case $d = 3$ a practical (actually working) algorithm for solving the equation (1) was proposed in the paper [5]. This algorithm is based on the *elementary version of Runge's method* for cubic diophantine equations firstly announced in [3]. In the next case $d = 4$, we also have a simple and elementary solving method which can be used instead of the classical Runge's method (see [4]).

In our paper, we consider a family of diophantine equations of the form

$$p(x,y)^2 + f_{\leqslant 3}(x,y) = 0, \tag{3}$$

where $p(x,y) \in \mathbb{Z}[x,y]$ is an irreducible quadratic form and $f_{\leqslant 3}(x,y) \in \mathbb{Z}[x,y]$ is a polynomial of degree at most three. Here we have $d = m = n = 4$ and each of the conditions (a), (b) (see Theorem of Runge) holds. Nevertheless, for some subfamily of such equations, Runge's method works (in other words, for the equation (3) the condition (c) may be violated sometimes). For comparison, going to apply Runge's method in the case $d = 3$, we can ignore the condition (c) for the following reason: if (c) is violated, then either (a) or (b) is violated necessarily.

The article is organized as follows. In Section 1, we give a sufficient condition which provides that the equation (3) has only a finite set of solutions over $\mathbb{Z}$ (Theorem 1). Also, we explain (including some examples) how one can verify the proposed condition in practice. In Section 2, we propose a practical algorithm for solving the equation (3) when our condition is satisfied. The mentioned algorithm is based on Theorem 2. Due to an additional parameter (the so-called *control parameter*), this algorithm admits an optimization.

1. Main theoretical result

Let
$$p(x,y) = Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x,y]$$
be a quadratic form in two variables. Suppose that $p(x,y)$ is irreducible over $\mathbb{Q}$ and consider the diophantine equation
$$p(x,y)^2 + f_{\leqslant 3}(x,y) = 0 \tag{4}$$
where $f_{\leqslant 3}(x,y) \in \mathbb{Z}[x,y]$ is a polynomial of degree at most three. We suppose that the polynomial in the left hand side of (4) is also irreducible over $\mathbb{Q}$. Denote
$$\Delta = B^2 - 4AC.$$

Clearly, in the case $\Delta < 0$ the algebraic curve defined by the equation (4) is bounded and this equation can be solved over $\mathbb{Z}$ by full search in the predetermined limits. Below we will assume $\Delta > 0$. The irreducibility of $p(x,y)$ means that Δ is not a perfect square in $\mathbb{Z}$.

In the following theorem we give a sufficient condition which provides the finiteness of the set of all solutions of the equation (4) over $\mathbb{Z}$.

Theorem 1. If the equation (4) admits the form
$$(p(x,y) + a_1x + b_1y)(p(x,y) + a_2x + b_2y) - dp(x,y) - a_3x - b_3y - c = 0, \tag{5}$$
where $(a_1, b_1) \neq (a_2, b_2)$, then the set of its solutions over $\mathbb{Z}$ is finite.

Proof. Let α be a root of the quadratic equation $p(1,y) = 0$. Consider the corresponding branch $y = \Psi(x)$ of the algebraic function defined by the equation (5). It is well known that the function $y = \Psi(x)$ can be represented as the Puiseux series (in particular, as the Laurent series) at $x = \infty$, namely
$$y = \Psi(x) = \alpha x + \beta x^{\varepsilon} + o(x^{\varepsilon}), \quad x \to \infty,$$
where $\beta \neq 0$ and $\varepsilon < 1$. Substituting $y = \alpha x + y_1$ in the equation (5), we obtain
$$\Delta x^2 y_1^2 + (\text{the summands of the form } \gamma x^i y_1^j) = 0,$$
where $i \leqslant 2$, $i + j \leqslant 4$ and $(i,j) \neq (2,2)$. We have $y_1 = \beta x^{\varepsilon} + o(x^{\varepsilon})$ as $x \to \infty$. So, in the case $\varepsilon > 0$ we lead to the following contradiction: the equality
$$\Delta \beta^2 x^{2+2\varepsilon} + (\text{the summands of the form } \gamma \beta^j x^{i+\varepsilon j}) + o(x^{2+2\varepsilon}) = 0$$
is impossible for all sufficiently large values of x. Thus, we have $\varepsilon \leqslant 0$. Consider two cases.

(I) The case $\varepsilon = 0$. We have

$$p(x,y) = \beta(B + 2C\alpha)x + o(x), \quad a_i x + b_i y = (a_i + b_i\alpha)x + O(1), \quad x \to \infty,$$

where $y = \Psi(x)$. Since α is irrational and $(a_1, b_1) \neq (a_2, b_2)$, the numbers

$$\gamma_i = \beta(B + 2C\alpha) + a_i + b_i\alpha \quad (i = 1,\, 2)$$

cannot be equal to zero simultaneously. Suppose $\gamma_1 \neq 0$. Then

$$\lim_{x\to\infty} \frac{dp(x,y) + a_3 x + b_3 y + c}{p(x,y) + a_1 x + b_1 y} = \frac{d\beta(B + 2C\alpha) + a_3 + b_3\alpha}{\gamma_1}. \tag{6}$$

Therefore, for large x, we get an additional equation

$$p(x,y) + a_2 x + b_2 y = w,$$

where w is an integer from a small neighborhood of the limit (6).

(II) The case $\varepsilon < 0$. We have $y = \alpha x + o(1)$ as $x \to \infty$. Then

$$p(x,y) = o(x), \quad a_i x + b_i y = (a_i + b_i\alpha)x + o(1), \quad x \to \infty.$$

We can assume that $a_1 + b_1\alpha \neq 0$. Hence,

$$\lim_{x\to\infty} \frac{dp(x,y) + a_3 x + b_3 y + c}{p(x,y) + a_1 x + b_1 y} = \frac{a_3 + b_3\alpha}{a_1 + b_1\alpha}. \tag{7}$$

Thus, for large x, we obtain an additional equation

$$p(x,y) + a_2 x + b_2 y = w,$$

where w is an integer from a small neighborhood of the limit (7).

As a result, in both cases (I) and (II) we reduce the diophantine equation (5) to a system of two algebraic equations. It is easy to see that such system has only a finite set of solutions. This completes the proof. □

Remark 1. Using the special variable z given by (10) and eliminating the variable y, we reduce the equation (5) to the equation

$$z^2(A_1 x^2 + (B(b_1 - b_2) - 2C(a_1 - a_2))xz + Cz^2) + F_{\leqslant 3}(x,z) = 0, \tag{8}$$

where $F_{\leqslant 3}(x,z) \in \mathbb{Z}[x,z]$ is a polynomial of degree at most three. We have

$$A_1 = A(b_1 - b_2)^2 - B(a_1 - a_2)(b_1 - b_2) + C(a_1 - a_2)^2.$$

Since $(a_1, b_1) \neq (a_2, b_2)$, we conclude that $A_1 \neq 0$. One can prove that any equation of the type (8) has only a finite set of solutions $(x,z) \in \mathbb{Z}^2$ (for detailed information, see [4]). This gives an another elementary proof of Theorem 1.

How to verify whether the equation (4) can be transformed to the form (5)? Let

$$f_{\leqslant 3}(x,y) = f_3(x,y) + f_2(x,y) + \ldots,$$

where $f_3(x, y)$ and $f_2(x, y)$ are the cubic and quadratic form, respectively. Clearly, the necessary condition is that $f_3(x, y)$ is divisible by $p(x, y)$. Suppose this condition satisfied. Then

$$l_1(x, y) + l_2(x, y) = l(x, y),$$

where $l(x, y) = f_3(x, y)/p(x, y)$ is the known linear form and

$$l_i(x, y) = a_i x + b_i y \quad (i = 1,\, 2)$$

are the unknowns linear forms. Further, we use the quadratic form $f_2(x, y)$. We have

$$f_2(x, y) = l_1(x, y)(l(x, y) - l_1(x, y)) - dp(x, y).$$

This is a quadratic equation with respect to the unknown linear form $l_1(x, y)$. Its discriminant

$$D(x, y) = l(x, y)^2 - 4(f_2(x, y) + dp(x, y))$$

must be a square of linear form over $\mathbb{Q}$ (in fact, over $\mathbb{Z}$). Consequently, the discriminant of the quadratic form $D(x, y)$ must be equal to zero. This gives a quadratic equation with respect to the unknown coefficient d, and we need only to solve it over $\mathbb{Z}$.

Example 1. Transform the equation

$$(x^2 - xy - y^2)^2 - 2x^3 + 2x^2 y + 2y^2 x + xy - 3y^2 - y = 0$$

to the form (5). Here we have

$$p(x, y) = x^2 - xy - y^2, \quad f_3(x, y) = -2x^3 + 2x^2 y + 2y^2 x, \quad f_2(x, y) = xy - 3y^2,$$
$$l(x, y) = \frac{f_3(x, y)}{p(x, y)} = -2x,$$
$$D(x, y) = (4 - 4d)x^2 + (4d - 4)xy + (12 + 4d)y^2.$$

For the coefficient d, we obtain the equation

$$(4d - 4)^2 - 4(4 - 4d)(12 + 4d) = 0,$$

which implies $d = 1$ or $d = -11/5$. Taking $d = 1$, we get $D(x, y) = (4y)^2$. Finally, the required form is

$$(p(x, y) - x + 2y)(p(x, y) - x - 2y) - p(x, y) - y = 0.$$

Example 2. Show that the equation

$$(y^2 - 2x^2)^2 - 3y^2 - x - y = 0$$

cannot be transformed to the form (5). Indeed, taking $p(x, y) = y^2 - 2x^2$, we obtain

$$D(x, y) = 8dx^2 + (12 - 4d)y^2.$$

Hence, $d = 0$ or $d = 3$, but in both cases $D(x, y)$ is not a square of linear form over $\mathbb{Q}$.

Now we discuss the question on finding the coefficient β. Using a computer algebra system, one can show that β is equal to one of the numbers

$$\beta_i = \frac{-Ba_i + 2Ab_i + (-2Ca_i + Bb_i)\alpha}{\Delta} \quad (i = 1,\, 2).$$

Suppose that $\beta = \beta_2 \neq 0$. Then

$$\begin{aligned}\gamma_2 &= \beta_2(B + 2C\alpha) + a_2 + b_2\alpha = 0,\\ \gamma_1 &= \beta_2(B + 2C\alpha) + a_1 + b_1\alpha = (a_1 - a_2) + (b_1 - b_2)\alpha \neq 0.\end{aligned}$$

In particular, $\beta_2(B + 2C\alpha) = -a_2 - b_2\alpha$ and we conclude that the limit (6) is equal to

$$w_\alpha = \frac{(a_3 - da_2) + (b_3 - db_2)\alpha}{(a_1 - a_2) + (b_1 - b_2)\alpha}. \tag{9}$$

For any $i = 1, 2$, it is not difficult to see that the equality $\beta_i = 0$ is equivalent to the equality $(a_i, b_i) = (0, 0)$. In the case $\beta_2 = 0$, the expression in the right hand side of (9) reduce to the most simple expression

$$\frac{a_3 + b_3\alpha}{a_1 + b_1\alpha}.$$

2. Solving algorithm and its optimization

In this section, we propose a simple practical algorithm for solving the equation (5) and we give several illustrative examples.

The main our problem can be formulated as follows: give explicitly a such condition on the solution $(x, y) \in \mathbb{R}^2$ of (5) that provides that the values of the expression

$$p(x, y) + a_2x + b_2y$$

turn out to be near the limit (9).

We can use that the curve defined by (5) admits a convenient parametrization (of course, non-rational because this curve is elliptic always). We introduce the parameter

$$z = p(x, y) + a_1x + b_1y. \tag{10}$$

After substitution $z - a_1x - b_1y$ instead of $p(x, y)$ in (5), we obtain the linear (with respect to x and y) equation

$$\omega_y(z)x + \omega_x(z)y + z^2 - dz - c = 0$$

with the coefficients

$$\omega_x(z) = (b_2 - b_1)z + db_1 - b_3, \quad \omega_y(z) = (a_2 - a_1)z + da_1 - a_3.$$

Hence, one can express y in terms of x and plug this expression into the equation (10). Thus, we obtain a quadratic equation with respect to x which can be solved (actually, we get the equation (8) rewritten in the corresponding form). After all, we get a parametrization for the equation (5) of the type

$$x = X_\pm(z), \quad y = Y_\pm(z),$$

where the expressions $X_\pm(z)$ and $Y_\pm(z)$ have the form

$$X_\pm(z) = -\frac{\eta_x(z)}{2\xi(z)} \pm \frac{\omega_x(z)}{2}\sqrt{\frac{\rho(z)}{\xi(z)^2}}, \quad Y_\pm(z) = -\frac{\eta_y(z)}{2\xi(z)} \mp \frac{\omega_y(z)}{2}\sqrt{\frac{\rho(z)}{\xi(z)^2}}.$$

Here $\xi(z)$, $\rho(z)$, $\eta_x(z)$, and $\eta_y(z)$ are the polynomials with integer coefficients, but we do not provide here their explicit expressions which are quite large. We only remark that $\deg \eta_x(z) \leqslant 3$, $\deg \eta_y(z) \leqslant 3$, and

$$\xi(z) = A_1z^2 + B_1z + C_1, \quad \rho(z) = \Delta z^4 + \dots,$$

where the coefficient $A_1 \neq 0$ is given in Remark 1. Furthermore, we have

$$w = p(x,y) + a_2x + b_2y = z + (a_2 - a_1)x + (b_2 - b_1)y = W_\pm(z),$$

where

$$W_\pm(z) = -\frac{\eta_w(z)}{2\xi(z)} \pm \frac{\omega}{2}\sqrt{\frac{\rho(z)}{\xi(z)^2}}$$

with $\deg \eta_w(z) \leqslant 2$ and the constant

$$\omega = \omega_x(z)(a_2 - a_1) - \omega_y(z)(b_2 - b_1) = a_3(b_2 - b_1) - b_3(a_2 - a_1) + d(a_2b_1 - a_1b_2).$$

Also, we note that the discriminant of the quadratic polynomial $\xi(z)$ is

$$\Delta_1 = B_1^2 - 4A_1C_1 = \omega^2\Delta.$$

Firstly, we consider the special case $\omega = 0$. In this case, we can find the rational coefficients d_1, d_2 and $c_1 \neq 0$ such that the equation (5) can be rewritten as

$$(p(x,y) + a_1x + b_1y + d_1)(p(x,y) + a_2x + b_2y + d_2) = c_1. \tag{11}$$

For instance, if $a_1 \neq a_2$ then we can set

$$d_1 = \frac{da_1 - a_3}{a_2 - a_1}, \quad d_2 = \frac{da_2 - a_3}{a_1 - a_2}, \quad c_1 = d_1d_2 + c$$

It is clear how we can solve the equation (11). Assuming $a_1 \neq a_2$ again, we rewrite it in the form

$$w = \frac{(da_2 - a_3)z + c(a_2 - a_1)}{(a_2 - a_1)z + da_1 - a_3}. \tag{12}$$

Then we find all the pairs $(z, w) \in \mathbb{Z}^2$ which satisfy (12) (they form a finite set). Finally, for all such pairs (z, w), we need to solve over $\mathbb{Z}$ the systems of the form

$$\begin{cases} p(x,y) + a_1x + b_1y = z, \\ p(x,y) + a_2x + b_2y = w. \end{cases}$$

For this, we eliminate $p(x, y)$ that leads to a linear equation with respect to x and y.

Further, we assume that $\omega \neq 0$. Let us consider two illustrative examples.

Example 3. Solve the equation

$$(y^2 - 2x^2)^2 - 2y^2 - x - y = 0,$$

which can be transformed to the form (5), namely

$$(y^2 - 2x^2 - 2x)(y^2 - 2x^2 + 2x) - 2(y^2 - 2x^2) - x - y = 0.$$

Here, we can take $z = y^2 - 2x^2 - 2x$ and $w = y^2 - 2x^2 + 2x$. Then we have

$$w = W_\pm(z) = \frac{12z^2 - 17z + 4}{16z^2 - 40z + 23} \mp 4\sqrt{\frac{2z^4 - 6z^2 + 3z + 1}{(16z^2 - 40z + 23)^2}}.$$

It is easy to see that

$$\lim_{z\to\infty} W_\pm(z) = \frac{3 \mp \sqrt{2}}{4}.$$

One can show that if $z \leqslant -2$ or $z \geqslant 2$ then the inequalities

$$0 < W_+(z) < 1$$

hold. Also, we have the inequalities

$$1 < W_-(z) < 2$$

when $z \leqslant -16$ or $z \geqslant 4$. Thus, any solution (x, y) can be written as $(X_\pm(z), Y_\pm(z))$ where

$$X_\pm(z) = \frac{-4z^3 + 13z^2 - 10z + 1}{16z^2 - 40z + 23} \mp \sqrt{\frac{2z^4 - 6z^2 + 3z + 1}{(16z^2 - 40z + 23)^2}},$$

$$Y_\pm(z) = \frac{-2z^2 + 8z - 5}{16z^2 - 40z + 23} \mp (4z - 5)\sqrt{\frac{2z^4 - 6z^2 + 3z + 1}{(16z^2 - 40z + 23)^2}}.$$

Taking $z \in \{-1, 0, 1\}$, we find all solutions of the form $(X_+(z), Y_+(z))$, namely

$$(0, 0) = (X_+(0), Y_+(0)), \quad (0, -1) = (X_+(1), Y_+(1)).$$

All solutions of the form $(X_-(z), Y_-(z))$ can be found if we take $z \in \{-15, -14, \ldots, 2, 3\}$:

$$(4, -5) = (X_-(-15), Y_-(-15)), \quad (0, -1) = (X_-(1), Y_-(1)).$$

Finally, the set of all solutions is $\{(0, 0), (0, -1), (4, -5)\}$.

Example 4. Consider the equation

$$(y^2 - 2x^2)(y^2 - 2x^2 + x) + y - c = 0 \tag{13}$$

with the integer parameter $c > 1$. Here, we have

$$z = y^2 - 2x^2, \quad w = y^2 - 2x^2 + x,$$

$$W_\pm(z) = \frac{(c-2)z}{z^2 - 2} \pm \sqrt{\frac{2z^4 + z^3 - 4cz^2 - 2z + 2c^2}{(z^2 - 2)^2}},$$

$$X_\pm(z) = \frac{-z^3 + cz}{z^2 - 2} \pm \sqrt{\frac{2z^4 + z^3 - 4cz^2 - 2z + 2c^2}{(z^2 - 2)^2}},$$

$$Y_\pm(z) = \frac{2z^2 - 2c}{z^2 - 2} \mp z\sqrt{\frac{2z^4 + z^3 - 4cz^2 - 2z + 2c^2}{(z^2 - 2)^2}}.$$

In particular,

$$\lim_{z \to \infty} W_\pm(z) = \pm\sqrt{2}.$$

One can prove that if

$$z \notin I_-(c) = \left[\frac{-4c + 9 - \sqrt{8c^2 - 72c + 145}}{4}, \frac{2c - 5 + \sqrt{8c^2 - 20c + 17}}{2}\right]$$

then the inequalities

$$-2 < W_-(z) < -1$$

hold and, similarly, if

$$z \notin I_+(c) = \left[\frac{-2c+3-\sqrt{8c^2-12c+1}}{2}, \frac{4c-7+\sqrt{8c^2-56c+113}}{4}\right]$$

then the inequalities

$$1 < W_+(z) < 2$$

hold. Thus, for all integer solutions $(x, y) = (X_\pm(z), Y_\pm(z))$ we have $z \in I_\pm(c)$. Relying on this claim, we can suggest an obvious algorithm for solving the equation (13).

Furthermore, investigating the expressions $X_\pm(z)$ and $Y_\pm(z)$ for $z \in I_\pm(c)$, we obtain the following upper bound for the solutions (x, y):

$$\max\{|x|, |y|\} < M_1 c, \tag{14}$$

where $M_1 > 0$ is an absolute constant (for instance, we can take $M_1 = 10$). We remark that the estimate (14) can be achieved (up to an absolute constant factor) for infinitely many values of c. Indeed, let (x_j, y_j) be the pairs of positive integers satisfying

$$y_j^2 - 2x_j^2 = -1$$

(it is well known from the theory of *Pell's equations* that there are infinitely many these pairs). Hence, for $c = y_j - x_j + 1$ the equation (13) has the solution $(x, y) = (x_j, y_j)$ for which

$$\max\{|x|, |y|\} \sim (2+\sqrt{2})c, \quad c \to \infty.$$

Before returning to the general case, let us consider Example 4 from the point of view of the effectiveness of used solving algorithm. Obviously, the proposed algorithm require $O(c)$ tests for the integer values of the expressions $X_\pm(z)$ and $Y_\pm(z)$ when the integer variable z runs through the intervals $I_\pm(c)$. Moreover, we can exploit directly the estimate (14) for solving the equation (13) by brute force. Fortunately, we can elaborate a more efficient solving algorithm. Rewrite $W_\pm(z)$ as

$$W_\pm(z) = \frac{(c-2)z}{z^2-2} \pm \sqrt{2} \cdot \sqrt{1 + \frac{z-4(c-2)}{2(z^2-2)} + \frac{(c-2)^2}{(z^2-2)^2}}.$$

We have

$$|W_\pm(z) \mp \sqrt{2}| \leqslant \frac{(c-2)|z|}{|z^2-2|} + \sqrt{2} \cdot \left|\sqrt{1 + \frac{z-4(c-2)}{2(z^2-2)} + \frac{(c-2)^2}{(z^2-2)^2}} - 1\right| \leqslant$$
$$\leqslant \frac{(c-2)|z|}{|z^2-2|} + \sqrt{2} \cdot \sqrt{\frac{|z|+4(c-2)}{2|z^2-2|} + \frac{(c-2)^2}{(z^2-2)^2}}$$

(for the last inequality, we use that

$$|\sqrt{1+t} - 1| \leqslant \sqrt{|t|} \tag{15}$$

for any $t \geqslant -1$). Hence, for given $m > \sqrt{2}$, if $|z| > m$ then

$$|W_\pm(z) \mp \sqrt{2}| < \frac{(c-2)m}{m^2-2} + \sqrt{2} \cdot \sqrt{\frac{m+4(c-2)}{2(m^2-2)} + \frac{(c-2)^2}{(m^2-2)^2}} = Q(m).$$

$\#(x, y)$	$\#c$
0	95957
1	3823
2	199
3	14
4	5
5	0
6	1

Table 1: The number of solutions of the equation (13) when $1 < c \leqslant 10^5$.

It is easy to see that $Q(\sqrt{c}) \sim \sqrt{c}$ as $c \to \infty$. Thus, we can conclude that the inequality

$$|z| > \sqrt{c}$$

implies the estimate

$$|w| = |W_{\pm}(z)| < M_2\sqrt{c}$$

with an absolute constant $M_2 > 0$ that is close to 1. Therefore, it is sufficient only $O(\sqrt{c})$ such tests for the expressions $X_{\pm}(z)$, $Y_{\pm}(z)$ and the similar expressions $\widetilde{X}_{\pm}(w)$, $\widetilde{Y}_{\pm}(w)$ which can be obtained by replacing $(a_1, b_1) \leftrightarrow (a_2, b_2)$ and $z \leftrightarrow w$ in $X_{\pm}(z)$, $Y_{\pm}(z)$. In our case, we have

$$\widetilde{X}_{\pm}(w) = \frac{2w^3 - 2cw - 1}{2(w^2 - 2)} \pm \frac{1}{2}\sqrt{\frac{8w^4 - 16cw^2 + (4c - 8)w + 8c^2 + 1}{(w^2 - 2)^2}},$$

$$\widetilde{Y}_{\pm}(w) = \frac{4w^2 - w - 4c}{2(w^2 - 2)} \pm \frac{w}{2}\sqrt{\frac{8w^4 - 16cw^2 + (4c - 8)w + 8c^2 + 1}{(w^2 - 2)^2}}.$$

As a result, we propose the following faster solving algorithm for the equation (13):

(a) find the integer values of $X_{\pm}(z)$, $Y_{\pm}(z)$ for all integers z satisfying $|z| \leqslant \sqrt{c}$, and

(b) find the integer values of $\widetilde{X}_{\pm}(w)$, $\widetilde{Y}_{\pm}(w)$ for all integers w with $|w| < M_2\sqrt{c}$.

For example, using this algorithm, we can solve the equation (13) for $1 < c \leqslant 10^5$ (see Table 1 which contains a statistical information on the number of solutions).

In the general case, we can proceed similarly. Let $m_0 = \omega\sqrt{\Delta}$ and

$$w_{\pm} = \lim_{z \to \infty} W_{\pm}(z).$$

Note that $\{w_{\pm}\} = \{w_{\alpha}\}$ where the numbers w_{α} are given by (9).

Theorem 2. Assume $m > |m_0|$. If

$$\left|z + \frac{B_1}{2A_1}\right| > \frac{m}{2|A_1|} \quad \text{or} \quad \left|z + \frac{B_1}{2A_1}\right| < \frac{2|m_0| - m}{2|A_1|}$$

then the estimates $|W_{\pm}(z) - w_{\pm}| < Q(m)$ hold. Here

$$Q(m) = \frac{|Q_1|m + |Q_2|}{m^2 - m_0^2} + \frac{|m_0|}{2|A_1|}\sqrt{\frac{|Q_3|m + |Q_4|}{m^2 - m_0^2} + \frac{|Q_5|m + |Q_6|}{(m^2 - m_0^2)^2}} \tag{16}$$

with the coefficients $Q_1, \ldots, Q_6$ expressed in terms of the coefficients of the equation (5).

Proof. We will use the variable

$$l = 2A_1 z + B_1$$

instead of z. In terms of l, we have the constraints $|l| > m$ or $|l| < 2|m_0| - m$. Also, we have

$$\xi(z) = \frac{l^2 - m_0^2}{4A_1}.$$

As a result, $W_\pm(z)$ can be rewritten as

$$W_\pm(z) = \frac{k_1 l^2 + k_2 l + k_3}{l^2 - m_0^2} \pm \frac{m_0}{2|A_1|} \sqrt{\frac{l^4 + k_4 l^3 + k_5 l^2 + k_6 l + k_7}{(l^2 - m_0^2)^2}}$$

with some coefficients $k_1, \ldots, k_7$. In particular, we have

$$w_\pm = k_1 \pm \frac{m_0}{2|A_1|}.$$

Thus, we obtain

$$W_\pm(z) - w_\pm = \frac{k_2 l + k_3 + k_1 m_0^2}{l^2 - m_0^2} \pm \frac{m_0}{2|A_1|} \left(\sqrt{\frac{l^4 + k_4 l^3 + k_5 l^2 + k_6 l + k_7}{(l^2 - m_0^2)^2}} - 1 \right) =$$
$$= \frac{Q_1 l + Q_2}{l^2 - m_0^2} \pm \frac{m_0}{2|A_1|} \left(\sqrt{1 + \frac{Q_3 l + Q_4}{l^2 - m_0^2} + \frac{Q_5 l + Q_6}{(l^2 - m_0^2)^2}} - 1 \right).$$

This representation (together with the inequality (15)) implies the estimate

$$|W_\pm(z) - w_\pm| \leqslant \frac{|Q_1||l| + |Q_2|}{|l^2 - m_0^2|} + \frac{|m_0|}{2|A_1|} \sqrt{\frac{|Q_3||l| + |Q_4|}{|l^2 - m_0^2|} + \frac{|Q_5||l| + |Q_6|}{(l^2 - m_0^2)^2}}.$$

Now, we can finish in the same way as in the proof of Theorem 1.1 from [5]. □

In practice, the solving algorithm based on Theorem 2 can be optimized in the same way as in the paper [5]: the control parameter m must be chosen so that the value of the corresponding *cost-function* $P(m) + Q(m)$ is minimal, where

$$P(m) = \begin{cases} \dfrac{2(m - |m_0|)}{2|A_1|}, & \text{if } m \leqslant 2|m_0|, \\ \dfrac{m}{2|A_1|}, & \text{if } m > 2|m_0|. \end{cases}$$

and $Q(m)$ is defined by (16). We demonstrated already one of examples of such an optimization (namely, for the case of the equation (13)). In the general case, the optimal value of m can be found using any standard numerical method.

References

[1] M.Ayad, Sur le théorème de Runge, *Acta Arith.*, **58**(1991), 203–209.

[2] L.J.Mordell, Diophantine equations, London, Academic Press Inc., 1969.

[3] N.N.Osipov, The elementary version of Runge's method for cubic equations, *Matematika v Shkole*, **1**(2012), 64–69. (In Russian)

[4] N.N.Osipov, Runge's method for the equations of fourth degree: an elementary approach, Matematicheskoe Prosveshchenie, Ser. 3, Vol. 19, MCCME, Moscow, 2015, 178–198. (In Russian)

[5] N.N.Osipov, B.V.Gulnova, An algorithmic implementation of Runge's method for cubic diophantine equations, *J. Sib. Fed. Univ. Math. Phys.*, **11**(2018), no. 2, 137–147.

[6] D.Poulakis, A simple method for solving the diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$, *Elem. Math.*, **54**(1999), 32–36.

[7] C.Runge, Ueber ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen, *J. reine und angew. Math.*, **100**(1887), 425–435.

[8] A.Sankaranarayanan, N.Saradha, Estimates for the solutions of certain diophantine equations by Runge's method, *Int. J. Number Theory*, **4**(2008), 475–493.

[9] V.G.Sprindžuk, Classical Diophantine Equations, New York, Springer-Verlag, 1993.

[10] Sz.Tengely, On the Diophantine equation $F(x) = G(y)$, *Acta Arith.*, **110**(2003), 185–200.

[11] P.G.Walsh, A quantitative version of Runge's theorem on diophantine equations, *Acta Arith.*, **62**(1992), 157–172.

Элементарный алгоритм для решения диофантова уравнения четвертой степени с условием Рунге

Николай Н. Осипов, Мария И. Медведева

Предлагается элементарный алгоритм решения диофантова уравнения

$$(p(x,y) + a_1x + b_1y)(p(x,y) + a_2x + b_2y) - dp(x,y) - a_3x - b_3y - c = 0 \qquad (*)$$

степени четыре, где $p(x,y)$ *обозначает неприводимую квадратичную форму положительного дискриминанта и* $(a_1, b_1) \neq (a_2, b_2)$. *Последнее условие гарантирует, что уравнение* $(*)$ *может быть решено с помощью хорошо известного метода Рунге, однако мы предпочитаем не использовать разложения в ряды, которые приводят к верхним границам для решений, бесполезным для компьютерной реализации.*

Ключевые слова: диофантовы уравнения, элементарная версия метода Рунге.